SPYWOLF

Security Audit Report

Completed on

February 04, 2023

OVERVIEW

This audit has been prepared for **North Apes** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

North Apes

PROJECT DESCRIPTION

According to their whitepaper:

North Apes is an interactive NFT collection of 5,555 unique apes and a deflationary token on the Ethereum blockchain. Both the NFT and the token come with well known but also new features and opportunities to take profits on an initial investment. Most importantly, however, does the project aim to incentivize activity along its community.

Release Date: Minting starts in February 3rd, 2023

Category: NFT

CONTRACT INFO

Token Name	Symbol
North Coin	NORTH

Contract Address
0x756A4837BB3ff544d9132d2067E44f40A2f10Ae2

Network	Language
Ethereum	Solidity

Deployment Date	Verified?
Feb 03, 2023	Yes

Total Supply	Status
1,000,000,000	Not launched

TAXES

Buy Tax
Up to 5%

Sell Tax
Up to 20%

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	1000000000 NORTH
Median Transfer Amount	1000000000 NORTH
Average Transfer Amount	1000000000 NORTH
First transfer date	2023-02-03
Last transfer date	2023-02-03
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-02-03 18:43:11 UTC
Created	2023-02-03 18:43:11 UTC
Create TX	0x4ed462b186a734fa0ec04de0ccf23832a1fe559357685c0e7560b96fc6490369
Creator	0x069c853983de5b78f103710d88681a7ca161f5d0

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Owner can withdraw LP tokens from the contract 2 days after initiating the unlockLP function.

```
uint256 private constant TIMELOCK = 2 days;

function unlockLP() external onlyOwner {
  _lpUnlockTimestamp = block.timestamp + TIMELOCK;
  emit UnlockLP(_lpUnlockTimestamp);
}

function withdrawLP() external onlyOwner {
  require(_lpUnlockTimestamp != 0 && block.timestamp >= _lpUnlockTimestamp,
  "NorthCoin::withdrawLP: LP is locked");
  IUniswapV2Pair pair = IUniswapV2Pair(_pair);
  uint256 lp = pair.balanceOf(address(this));

  if (lp != 0) {
    pair.transfer(_pair, lp);
    pair.burn(address(this));
  }

  IERC20 weth = IERC20(_weth);
  weth.safeTransfer(_treasury, weth.balanceOf(address(this)));
 }
}
```

FOUND THREATS

Informational

This token uses dynamic sell fees up to 20%.
Buy fees are from 5% to 1% considering the amount of NFTs that user hold (from 0 to 4 NFTS). If user holds above 4 nfts buy fees become 0%.
Combined buy+sell=25%.

```
function _transfer(address sender, address recipient, uint256 amount) internal override {
.........................
    uint256 fee;
    buying = true;
  uint256 balance = IERC721(_nft).balanceOf(recipient);

  if (balance == 0) {
    fee = amount / 20; // 5%
  } else if (balance == 1) {
    fee = amount / 25; // 4%
  } else if (balance == 2) {
    fee = amount * 3 / 100; // 3%
  } else if (balance == 3) {
    fee = amount / 50; // 2%
  } else if (balance == 4) {
    fee = amount / 100; // 1%
  }
}
} else if (recipient == _pair) { // selling
uint256 newVariableSellFee = Math.min(variableSellFee + FEE_DENOMINATOR * amount / liquidity, FEE_DENOMINATOR / 5);
// increase variable sell fee based on amount vs liquidity to max. 20%

if (newVariableSellFee != variableSellFee) {
  emit UpdateVariableSellFee(variableSellFee, newVariableSellFee);
  variableSellFee = newVariableSellFee;
}

fee = amount * variableSellFee / FEE_DENOMINATOR;
}
.........................
}
```

FOUND THREATS

Informational

This contract uses intermediary 'treasury' contract that sets the token's router and receives the total minted token supply and NFT contract that is used in dynamic buy taxes functionality.
The intermediary and the NFT contracts are not in the scope of the current audit.

```
address private immutable _treasury;
address private immutable _nft;
address private immutable _router;
address private immutable _weth;
address private immutable _pair;

constructor(address treasury, address nft) ERC20("North Coin", "NORTH") {
  _treasury = treasury;
  _nft = nft;
  _router = INorthTreasury(treasury).router();
  IUniswapV2Router02 router = IUniswapV2Router02(_router);
  _weth = router.WETH();
  _pair = IUniswapV2Factory(router.factory()).createPair(address(this), _weth);
  _mint(treasury, 10 ** decimals() * MAX_SUPPLY);
  _updateHolders(treasury);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

North Apes

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot set a transaction limit
- ✔ The smart contract utilizes "Math" to prevent overflows

TOKENOMICS

The following tokenomics are based on the project's whitepaper:

The maximum supply of North Coin is minted to the treasury during token contract creation and remains reserved for the initial liquidity pair (NORTH/WETH) on Uniswap.

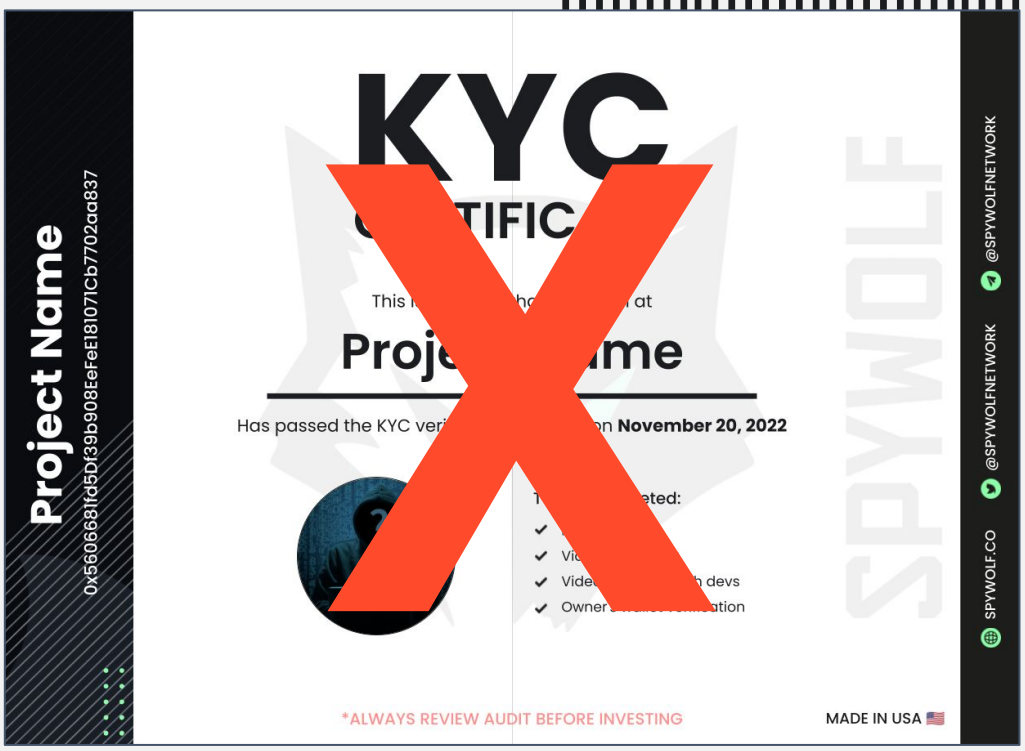
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://northapes.com/

Domain Registry
https://www.namecheap.com

Domain Expiration
Expires on 2024-01-23

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design, nice color scheme and appropriate graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes

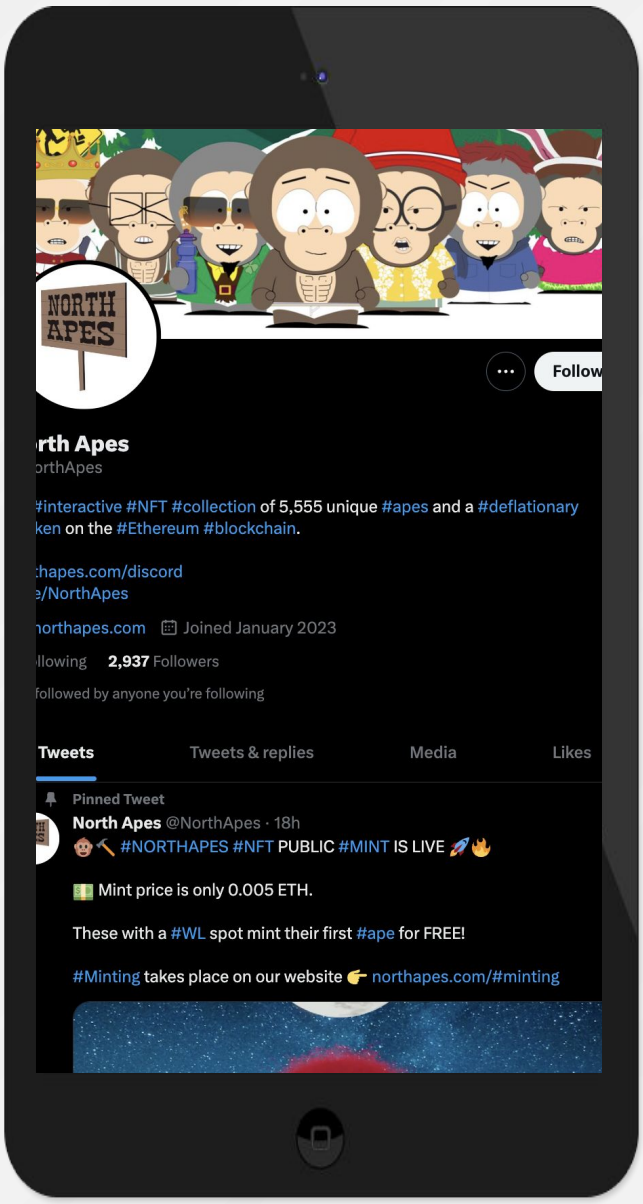
northapes.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Social media channels are active with organic users, mainly concentrated in discord.



Twitter

@NorthApes

- 2 979 followers
- Posts frequently
- Active

Discord

https://discord.com/invite/f47QeY76Pe

- 4 343 members
- Active members
- Active mods

Telegram

@TelegramUSERNAME

- 27 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.